Los Alamos
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

center for computer security

DRAFT

October 22, 1982

STAT

Dear Bob:

In response to your letter of 22 September, I think we are in general agreement about how to proceed on Project Venerable. The questions you asked suggest you are thinking along the same lines we are. I'll address your questions in the order in which they were posed.

a. We presume there will be no physical damage to the equipment. However, we might want to consider temporarily attaching test equipment some special purpose hardware to the system. For example, we might want to consider building a box to try to exploit the known problem of how the master console is determined at power up. We might also want to break out the signals on the cables from the work station to the CPU to see if there is something in the protocol which could be exploited.

b. Our proposal for a continued low level effort is based on the idea that a system would be leased for installation at Los Alamos. You would put in some money toward the lease, and so would I. The system here would be configured to be like those you are most concerned about. That gives us both a system in daily operation where user experience will suggest possible problems. In addition, we would initiate a small effort to systematically work on the system. When a potential problem is suggested, by your local experience, by your Agency wide experience, or by our experience, we would evaluate the report to answer the following questions.

- Is there an actual vulnerability?
- How difficult is it to exploit the vulnerability?
- What countermeasures can be employed?

Your committed level of funding would cover your participation in the lease and development of systematic techniques for investigating systems for which little information is provided. Once a problem is identified we would estimate the effort and agree on additional funding to cover the analysis.

This arrangement has several advantages.

- It provides a longer look at the Wang system which increases the likelyhood that the system's problems will be found.
- It provides a capability for quickly assessing the seriousness of problems uncovered in the field.
- It may yield a method for examining computer systems about which little is known in advance.

c. Preliminary work to be done at Los Alamos would include analysis of available documentation, user training, and analysis of a disk pack.

- We want to review all of the documentation available on the system. ISSG would have to provide this information.
- We will try to obtain training time on a Wang system in Albuquerque.
- Analysis of this system will require understanding of the data structure on the disk. Assuming that the data structure is not described in detail in the documentation that is available, we would like to have ISSG build a disk that we can examine here. To do this, you would mount the pack and write a few files on it - any text. We would need the pack and details of the data such as the names of the files and printouts of the files themselves.
- We want to know as much as possible about the CPU to terminal protocol before we begin. This information will be obtained from existing documentation and from studying other Wang systems which we have available. We suppose that the terminal protocol will have changed at most very little from current systems.
- We will need a list of any optional software which will be

available on the system to be studied, and copies of the documentation that goes with it.

d. We envision this study as a team effort involving two Los Alamos people plus designated ISSG members. To prepare for the test, ISSG should do the following.

- Team members should review documentation while we are doing that here and should take available training courses from Wang.
- ISSG should set up two user accounts on the machine for our use when we arrive for the test. We would prefer that there be some files in these accounts.
- The system should not be used to process documents for which we do not have access until after the test has been completed. We do not know how good the disk erase software is (if there is any), and we may read the entire disk. You have to assume that we may see anything that is, or has been, on the system.

STAT e. [redacted]

f. To the extent possible specific recommendations for countermeasures to system vulnerabilities will be developed. Recommendations may be for mods by the vendor, configuration changes, or changes in procedures. We will probably not learn enough to be able to recommend patches to the software. Any recommendations should be worked out by the whole team - particularly procedural changes, where the ISSG team members will have the best ideas about the impact on users.

g. We think the system should be given some real usage before the test occurs. It would be quite helpful to have the test team include one of your secretaries - at least on a part time basis. Secretaries will likely be the most frequent users of the system, and hence will have the greatest opportunity to notice its peculiarities. You should get one or more working on the system soon and have them make a diary of all odd things that happen while they are using it.

h. None. The funds transfer memo we have is sufficient.

i. We have already begun. Both of us have vacation to use or lose by the end of December, so December will not be very active, but much of the preliminary work will be out of the way before then. We expect the actual test can be completed during January.

j. Involvement of ISSG personnel is essential to the success of this test. Roger an I are computer people who will not have had as much experience on the system as we would like when the test begins. We would like ISSG to involve at least one computer person - hopefully the one who has examined the code, one secretary who has experience using at least the word processing software, and someone who knows how the system will be used when it is deployed by the Agency.

The schedule will look approximately as follows.

- October 29. Preliminary meeting to discuss this letter and settle strategy questions.
- Week of November 1. Meeting between Los Alamos team members and selected other Los Alamos personnel to select areas to be tested and write preliminary test plan.
- Week of November 1. Selection of team members by ISSG. Meeting similar to that at Los Alamos with emphasis on listing questions that have to be answered before field deployment of the system. For example, "Can we allow the use of BASIC?"
- Remainder of November. Preliminaries as described in c and d above.
- Week of December 6. Full team meeting at ISSG (1-2 days) to write test plan.
- Last week in January. Execute test plan. May take two weeks including the writing of the report and selection of countermeasures.

I think this will be an exciting project. It is a big effort, but the results will be very useful. You should think about what sort of final report you wold like. Presumably, there will be a report that goes to the CSS, which we would like to be able to polish after we return home in January or February. Will there also be a version that is sent to Wang? Will there be a version that is limited to the Agency?

See you on October 29.

Sincerely,

David Bailey